

REMARKS

Claims 1-14 are currently pending in the case.

I. Objection to the Title

The examiner objected to the title. The title has been amended in accordance with the examiner's suggestion.

II. Objection to the Specification

The applicant has amended the specification regarding the informalities on pg. 9.

III. Rejections of Claims 1-5 and 9-14 under 35 U.S.C. 103 based on Schneier in view of Deo; and rejection of claims 6-8 under 35 U.S.C. 103 based on Schneier in view of Deo and asserted admitted prior art

The examiner has rejected claims 1-14 under 35 U.S.C. 103 based on Schneier in view of Deo and for some of the claims in view of asserted admitted prior art. The examiner's rejections, respectfully, are based on a series of leaps, the last and greatest of which, goes against the express teachings of Schneier. The applicant strenuously asserts that the examiner is incorrect, as will be further explained, and files a notice of appeal with this response to office action.

With regards to claim 1 the examiner states that:

- a. "... the method disclosed by Schneier is silent on the matter of encrypting a key value ."
- b. "... this encryption method disclosed by Schneier does not specify the step of generating a signature based on the triplet a(new), b(new) and E ."

- c. "Finally, Schneier is silent on the matter of the same random number c being used in the key encryption step and in the signature step."

The applicant respectfully asserts that the prior art does not suggest providing or combining the many items missing from the Schneier reference.

Regarding the "same random number c ", the examiner, respectfully, is completely wrong. Schneier is not silent on the matter of whether the same random number should be used in the key encryption step and in the signature step. Schneier is loud and clear in stating that one must not use the same random number in the encryption step and in the signature step:

"Each El Gamal signature or encryption requires a new value of k ; and that value must be chosen randomly." (Schneier, p. 477, third paragraph, second sentence, emphasis added).

The " k " of Schneier is the " c " described in the background of the present application. The "background" section of the present application states:

"El Gamal encryption is a standard method of encryption known in the art. In this method a first processor performing the encryption step, takes a message m as an input; chooses a random value " c ", and produces the outputs $a = m \cdot y^c$ modulo p ; $b = g^c$ modulo p . (Present application, paragraph two, first two sentences)."

The Schneier reference states:

"El Gamal Encryption ...

$$\begin{aligned} a &= g^k \text{ mod } p \\ b &= y^k M \text{ mod } p \end{aligned}$$

The pair, a and b , is the ciphertext" (Schneier, pg. 478, see also pg. 476).

The quantities a , b , and k , of Schneier correspond to the quantities b , a , and c , respectively, of the background of the present application.

Since " k " of Schneier is " c " as described in the background of the present application, the sentence in Schneier can be restated as:

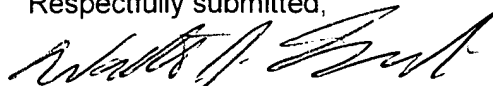
-- Each El Gamal signature or encryption requires a new value of c, and that value must be chosen randomly. - - (restatement of Schneier reference sentence with "c" substituted for "k", emphasis added)

Respectfully, there is no way one skilled in the art, or unskilled in the art, would ever choose the same value of c, based on the express teaching against doing so in Schneier. Claim 1 is respectfully submitted to be allowable for at least the above reasons. Claims 2-5, and 9-10 are dependent on claim 1 and are submitted to be allowable for at least the same reasons. Claims 6, 8, and 11 have a somewhat similar limitation regarding the same number c for encryption and signature and are submitted to be allowable. Claim 7 is dependent on claim 6, claims 12-14 are dependent on claim 11, and these claims are also submitted to be allowable.

V. Conclusion

Claims 1-14 are respectfully submitted to be in a condition for allowance. Favorable reconsideration of this application, as amended, is respectfully requested.

Respectfully submitted,



Walter J. Tencza Jr.
Reg. No. 35,708
Suite 3
10 Station Place
Metuchen, N.J. 08840
(732) 549-3007
Fax (732) 549-8486